



Overt Deployment of Live Facial Recognition (LFR) Technology Policy (Surrey and Sussex) (1249/2025)

Abstract

This policy describes how Surrey Police and Sussex Police Deploy Live Facial Recognition Technology.

Policy

1. Introduction

1.1 Live Facial Recognition (LFR) is used by Surrey Police and Sussex Police (hereafter referred to as the Forces) as a real-time deployment of facial recognition technology, which compares a live camera feed (or multiple feeds) of faces against a predetermined watchlist, in order to locate persons of interest by generating an alert when a possible match is found. More detail about how LFR works and how the Forces uses it can be found in section 3 (LFR Overview) and on the College of Policing website Live facial recognition | College of Policing

1.2 This LFR Policy provides the Force's personnel with advice on the overt use of LFR in a legally compliant and ethical manner to enable the Forces to achieve legitimate policing aims. (Overt means "apparent" or "visible." Covert means "hidden" or "concealed.")

1.3 The Forces are also cognisant of the views and ongoing considerations of the Information Commissioner, Biometrics and Surveillance Camera Commissioner and has participated in the development of national guidance and a code of practice relating to LFR and its use by UK Law Enforcement Agencies (LEA).

1.4 LFR is used by the Forces purely in an overt capacity.

1.5 This policy will reassure the public that the approach and decision making taken to support LFR deployment will be conducive to public confidence and mitigation against data accuracy concerns in our Crime Recording system.

2. Scope

2.1 This policy and procedure aims to provide the Force's personnel and members of the public with information about our strategic, operational and technological objectives for the overt use of LFR.

2.2 This policy and procedure will identify the governance structure for the deployment of LFR to offer sufficient assurances that the Force's use of LFR is appropriately governed and legally compliant.

3. Policy Statement

3.1 It is strongly advised that officers and staff adhere to the policy to ensure the lawful use of LFR to serve the public whilst providing necessary safeguards. It is also important to maintain the trust and confidence of the public as well as our partners and other stakeholders.

3.2 It is recognised that circumstances may arise where for valid reasons, a decision is taken that it is necessary to make changes outside of this policy for operational policing purposes. These decisions must be fully documented, together with detailed rationale and that the relevant decision-making features within debrief and evaluation processes.

Procedure

1. What is LFR?

1.1 This policy specifically addresses the deployment of LFR by the Forces. It does not include use of Retrospective Facial Recognition (RFR) or Operator Initiated Facial Recognition (OIFR) technology. RFR is often referred to as post-event, which relates to non-real time searching of images against a database. OIFR is where an officer takes a picture of a subject via a mobile device and submits it for immediate search (not currently deployed within the Forces).

1.2 LFR can be a valuable policing tool that helps Forces keep the public safe and to meet their statutory and common law policing duties, which include the prevention and detection of crime, the preservation of order, the bringing offenders to justice and wider safeguarding duties.

1.3 There is a reasonable expectation that personal information will be processed for the fulfilment of operational police duties including:

- Protection of life
- Preserving order
- Preventing the commission of offences, and
- Bringing offenders to justice
- Safeguarding duties.

2. Use of LFR

2.1 LFR is a real-time deployment of facial recognition technology, which compares live camera feed(s) of faces that appear within a set zone of recognition against a predetermined Watchlist by generating an alert to a human operator for review and consideration for further interventions when a Possible Match is confirmed.

2.2 The Watchlist will be compiled from images processed by Forces under the UK GDPR and Part 3 of the Data Protection Act 2018 depending on the purpose of each deployment. All images used for deployment will meet operational thresholds clearly detailed and recorded and authorised by the Forces.

2.3 Each watchlist is bespoke for every deployment and the rationale for the generation of the Watchlist must be intelligence led, justified, proportionate and necessary. The criteria for Watchlist constructs must be approved by the Authorising Officer (the 'AO') and be specific to an operation or to a defined policing objective. The AO will be any rank of Superintendent or above to ensure resilience in deployment of this resource (full details are available in the LFR Standard Operating Procedure).

2.4 Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the deployment.

2.5 The AO should define the date, time, location and duration the deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the deployment.

2.6 To ensure transparency of processing, members of the public will be informed prior to a deployment through publications on the Forces website / social media platforms. This publication should be made 7 days ahead of the deployment. There will be clear signage at all deployments to fully inform the public that LFR technology is active and provide further information should it be required.

2.7 Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence, and this is not justification to engage.

2.8 All deployments LFR will be recorded on a centrally held register that will be public facing on the Forces website. Following each LFR deployment, the Silver Commander must ensure that a post deployment evaluation is completed and updated in the Deployment Record.

3. Retention and Recording

3.1 The biometric templates and the actual CCTV footage captured during the deployment will be deleted at the end of the deployment (at the latest within 24 hours of the termination of the deployment). This is a necessary process to ensure compliance with the obligations to process data fairly proportionally and for no longer than is needed as well as to encourage the support of the public when deploying this tactic.

3.2 Engagement with the public following an LFR match will be recorded on Body Worn Video (BWV). This will be retained for a minimum of 30 days to support an investigation and also to allow for the exercising of data subjects Rights of Access.

4. Information Sharing / Data Protection

4.1 All processing of LFR deployment data is compliant with the requirements of DPA 2018 and UK GDPR. This is fully addressed under the Supporting Documents (Section 6).

4.2 Any data relevant for retention (such as the identification and subsequent arrest of a Wanted Person) will be processed and retained under the Forces statutory functions carried out by a competent authority for a law enforcement purpose.

4.3 LFR data will only be shared where necessary to support the law enforcement purpose, such as for prosecution purposes.

5. Training

5.1 LFR engagement officers will be briefed at the commencement of their shift to understand the LFR application, how it performs, and what effect any potential subject, system, and environmental factors might have on the success of the deployment.

5.2 LFR Operators receive training prior to any operational deployment and support of LFR technology.

5.3 All supporting officers will receive a full operational briefing prior to deployment and will be deployed in police uniform.

6. Supporting Documents

6.1

- LFR Legal Mandate – this details compliance with legislation for processing data in relation to LFR deployments.
- LFR Standard Operating Procedure (SOP) – this outlines measures relevant to considering when planning and deploying LFR technology. This also includes any additional considerations for the generation of the Watchlist.
- LFR DPIA – this details the nature, scope, context and purposes of LFR processing. It assesses the necessity, proportionality and compliance measures to reassure that Privacy By Design has been implemented at all stages of processing.
- LFR Appropriate Policy Documents – outlines how the processing of personal data is compliant with the requirements of the Data Protection Act 2018 and UK General Data Protection Regulations.